AO 106 (Rev. 04/10) Application for a Search Warrant HH

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple Iphone, model # MNAY2LL/A recovered from residence of Darren Kamnitzer, 699 Streamwater Drive, Blacklick, OH and currently held in FBI storage at 425 W. Nationwide Blvd, Columbus, Ohio

Case No. 2:19mj095

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Secs 2251(a) and (d)	Production of or advertising for child pornography in interstate commerce
18 USC Secs 2252 and 2252A	Receipt/possession of child pornography/visual depictions of minors engaged in sexually explicit conduct in interstate commerce
18 USC 2422(b)	Coercion/enticement of a minor to engage in illegal sexual activity

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brett M. Peachey, FBI TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/4/2019

Judge's signature

City and state: Columbus, Ohio

Elizabeth Preston Deavers, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No. 2:19mj095**
	)	
Apple Iphone, model # MNAY2LL/A recovered from the residence of Darren Kamnitzer, 699 Streamwater Drive Blacklick, Ohio 43004 and currently held in FBI storage at 425 W. Nationwide Blvd, Columbus, Ohio	)	**Magistrate Judge**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.

2. During my career as a police and task force officer, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography, including, but not limited to, the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.

3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the following digital media: Apple Iphone Model MNAY2LL/A (the SUBJECT MEDIA). The SUBJECT MEDIA was seized pursuant to the execution of a search warrant at the residence of Darren Kamnitzer, 699 Streamwater Drive, Blacklick, Ohio 43004. I have not withheld any evidence or information that would negate probable cause.

5. The SUBJECT MEDIA to be searched is more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – the production, advertising, distribution, transmission, receipt, and/or possession of child pornography, and the coercion or enticement of a minor to engage in illegal sexual activity.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means

or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly receive, distribute or possess any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. Title 18 USC § 2422(b) makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime, which includes the production of child pornography, as described in paragraph 6 above.

11. As it used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as:

> actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

12. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography" is defined in 18 U.S.C. § 2256(8) as: [1]

> any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

13. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

14. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10))

15. The following terms have the same meanings or explanations in both statutes:

A. "minor" means any person under the age of eighteen years (18 U.S.C. § 2256(1));

B. "visual depiction" includes undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format (18 U.S.C. § 2256(5));

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and the attachments hereto include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

C. "computer"[2] is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. . . " (18 U.S.C. §§ 1030(e)(1) and 2256(6)).

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, THE INTERNET AND TWITTER

16. Based on my training and experience, I use the following terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile/cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, modern wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital image files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any

2 The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

digital data, including data unrelated to photographs or videos. Most digital cameras also include a screen for viewing the stored images.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and observation of the device, I know that the SUBJECT MEDIA has abilities that allow it to serve as a mini handheld computer, electronic storage device, wireless telephone, digital camera, digital video recorder, portable media player, GPS navigation device, and to connect to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, where the device has been, and what messages were sent to or from the device via text message, e-mail, or other internet-based messaging applications.

18. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime; and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of the crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, instrumentalities of crime and/or fruits of crime.

19. Digital or electronic files or remnants of such files can be recovered months or even years

after they have been downloaded onto a hard-drive or other digital/electronic device and can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file on a digital device, the data contained in the files does not actually disappear; rather the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on the hard drive that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

20. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and usage habits.

21. Computers and mobile computing devices (smart phones, tablets, and electronic storage media, hereinafter referred to as "mobile devices" or "mobile computing devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or a mobile computing device with a built in camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

22. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

23. The capability of digital devices to store images in digital form makes them an ideal

repository for child pornography. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards which can add up to an additional 128 Gigabytes of storage. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

24. The development of computers and mobile devices has added to the methods used by child pornography collectors to interact with each other and with minors they seek to exploit. Computers and mobile devices serve four functions in connection with child pornography: production, communication, distribution, and storage.

25. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

26. These internet-based communication structures are ideal for the child pornography collector. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity, or to hide their true identity when seeking out minors online. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors, or to convince a child to produce and send such images or meet for the purpose of sexual activity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between collectors of child pornography.

27. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the methods of distributing child pornography. For example, child pornography can be transferred via electronic mail or messaging applications through file transfer protocols (FTP)[3] to anyone with access to a computer or a mobile device and Internet service. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer/mobile device is a preferred method of distribution of child pornographic materials.

28. A growing phenomenon related to smartphones and other mobile computing devices, such as tablets, is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include Kik messenger service, Snapchat, Twitter, and Instagram.

29. Twitter is an online news and social networking service on which users post and interact with messages knowns as "tweets." Users can access Twitter through its website interface, through Short Message Service (SMS) or its mobile-device application software or "app." Tweets are publicly visible by default but senders can restrict message delivery to just their followers.

---

3 The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP", allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

Users can tweet via the Twitter website, compatible external applications, such as smartphones, or by SMS. Users may subscribe to other users' tweets, known as "following" and subscribers are known as "followers." Individual tweets can be forwarded by other users to their own feed, a process known as a "retweet". Users can also "like" individual tweets. Twitter allows users to update their profile via their mobile phone either by text messaging or by apps released for certain smartphones and tablets. Twitter also offers direct messaging between users which are private and not visible to other users. In addition to text, users can include a photo or video with their direct message. Users can take a photo or record a video to send in a direct message or attach one from their device gallery.

30. Individuals can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Gmail, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or mobile device capable of accessing the Internet. Even in cases where online storage is used, however, evidence of the use of such storage account and/or child pornography can often be found on the user's computer, mobile computing device or external storage media.

31. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

32. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER AND MOBILE COMPUTING SYSTEMS

33. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. SEARCH METHODOLOGY TO BE EMPLOYED

35. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a

non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment A;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A;

c. surveying various files, directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

36. An additional search methodology referred to as "chip-off" will likely be used, due to the current functionality of the SUBJECT MEDIA. Specifically, this process is believed to be necessary because other traditional methods of forensic examination of the SUBJECT MEDIA have not been successful in obtaining any deleted data from the SUBJECT MEDIA. Chip-off forensics is an advanced digital data extraction and analysis technique which involves physically removing flash memory chip(s) from a device, and then acquiring the raw data using specialized equipment. Chip-off forensics is a powerful capability that allows Binary Intelligence to collect a complete physical image of nearly any device – even those which have suffered catastrophic damage. The Ohio Bureau of Criminal Investigation ("BCI") is currently one of the only forensic laboratories in Ohio that has the capability of conducting the chip-off process, and the SUBJECT MEDIA will be transported to BCI for this purpose. The chip-off process renders the cellular phone inoperable for any future use or examination. In this case, your affiant has significant reason to believe, based on the information obtained during the course of the investigation, that the SUBJECT MEDIA contains evidence of numerous child exploitation offenses, and that this evidence cannot be obtained using any other forensic examination method.

VII. INVESTIGATION AND PROBABLE CAUSE

37. On September 11, 2018, a subject utilizing the Twitter user name "Jacobauditions" contacted a ten year old female in Switzerland, hereinafter referred to as "MG," via Twitter's direct messaging function. Jacobauditions was posing as the manager for Jacob Sartorius, who is a teenage singer and internet personality in the United States, and asked MG if she would like to audition to be in a video with Sartorius. After being advised that MG was ten years of age, Jacobauditions asked her several background questions and then requested that she take a full length "selfie" of herself in the mirror. After receiving the photo, Jacobauditions gave details regarding how the video would be made and advised that she and a parent would be flown to California where the video would be produced if she could pass the audition.

38. After advising MG that the video would be produced on a beach, Jacobauditions requested that she take a photo of herself in a bikini and send it to him. After MG advised that she was not comfortable taking a photo of that nature due to her age, Jacobauditions asked her to be "brave" and "strong" advising "I know you can do this and no one is going to see this okay?"

39. MG agreed to take the photo but advised that she did not have a bikini. Jacobauditions advised her that a bra and underwear are the same and that many of the other fans who have auditioned for the video used a bra and underwear as well. When MG conceded to taking the photo, Jacobauditions instructed her that it has to be a full length photo and her shirt has to be lifted like a bikini. At that point, a photo was sent from MG to Jacobauditions. However, this photo could not be recovered in the conversation so its contents are unknown.

40. After MG sent this photo, Jacobauditions responded "There is only one more part and then we will be done and you will get to talk with Jacob then. I need to know you are 100% serious about this because we are investing a lot of money in this and in you. I need to know that when you are with Jacob that you can do what I ask when I ask. It will be the most difficult think (sic) you've ever had to do, but I know you are up to it. I need you to take one more picture, just like the last one you took, but with no top on at all. This picture will be deleted automatically 3 seconds after you message it, and no one will ever see it, ever. It will show that you are serious, and then we will be done. Be brave I know you can do this."

41. MG sent another photo and, after this photo was sent, Jacobauditions responded "ok good deleted, but it has to be the bottoms also" to which MG sent another photo. Jacobauditions advised that the photo "has to show the bottom as well" and "You don't have to show your face but it has to show down there." As MG continued to send photos, Jacobauditions responded "It

has to show between your legs, all those are deleted" and "closer .....I need you to sit on the bed, with your legs spread open, and picture in between your legs." All of the photos that MG sent during this part of the conversation could not be recovered and their content is unknown.

42. Jacobauditions then asked MG if she knows how to take a video and states "ok, there are only a few more pictures to take. I need a closer picture in between your legs, and I need you to open it up a little with your fingers." MG responded by sending a short close up video, nude from the waist down, of her vagina. Although the child's face is not visible and her chest area is clothed, there is no evidence of breast development or pubic hair, and she thus appears to be prepubescent. Jacobaudtions responded "ok, so I need you to do that again, but open it up a little more, for 20 seconds. And I want you to say that you love Jacob Satorius and want him to come to Switzerland…..and your shirt can't be on." MG responded by sending a twenty second video depicting a close up of her vagina using her fingers to expose herself. Jacobaudtions responded "you still have your shirt on, can you please do it again." MG responded with another twenty second video, without wearing her shirt, where she is using her fingers to spread and expose her vagina.

43. Jacobauditions then responded "ok good, we are getting close...you are doing so well. Next, and remember, all the others have done this. I need a 20 second video, I need to see your butt and the hole. I need you to point your butt at the camera and spread your cheeks so I can see inside." When MG responded "That is sexual abuse…I am ten years old I cannot do it," Jacobauditions assured her that it is all part of the audition and that all the other participants have done it. After additional encouragement, MG sends a sixteen second close up video of her vagina and anus. At one point in the video she rolls over onto her stomach in an attempt to record her buttocks.

44. Jacobauditions then advised "Okay, there is only one more and then we are done, but it is difficult, but I know you can do it….I need you to first, to set your phone down taking a video like you just did, and focus on your butthole like in thie (sic) picture for 15 seconds….I want you to be able to focus the video on that shot for 15 seconds, let's see if you can do that on the floor….remember, no clothes on at all." MG responded to these messages by sending a fifteen second video depicting a close up of her vagina. Jacobaudtions then responded "close, you need to be more over it, that wasn't your butt hole….if you just move a little more forward it will show it….you were close." After MG sent a fifteen second video depicting a close up of her anus and vagina, Jacobauditions responded "Perfect!"

45. Jacobauditions then wrote "okay, so the last video, what I need you to do....is it will be a little messy, so do it on the floor on a towel. But it needs to be a 30 second video, just like that one where you see your butthole the whole time, I want to see you poop and pee. I want to see it all come out. If you do this correctly we will be done 100%." When MG responded that she can't because she doesn't have to go to the bathroom, Jacobauditions replied "I want to see you try. I want to see your butthole push and your privates push to pee….I just need to see it all come out…from the holes." After MG responded by sending a fifteen second video which depicted herself urinating on a towel, Jacobauditions responded "ok good, but here is the deal. That is the perfect position, but I need you to lift your legs so your butthole is exposed. When you are ready to poop and pee again, I need you to take the 30 second video just like this one, and do both onto that towel….you are so close. The whole point is a close up of your butthole and private as the poop and pee come out. I want to actually see the holes open up and for it to come out. It needs to be close up and I need to see it. That was just a little so I need you to eat a lot, and save up, and take a really long video of the poop coming out okay….once that is done you will get all the time you want with Jacob." MG advised that she has tried multiple times but has not been able to defecate on camera for him. He then responded "ok, until you are ready to poop, one more video....all clothes off, legs spread as far apart as possible, camera in between your legs. Rub your privates up and down, and say ohhhhh Jacob several times. Do this for 40 seconds, and slowly get faster at the rubbing and talking." MG then sent a thirty five second close up video of herself urinating and defecating on a towel.

46. After this video is sent, Jacobauditions continued to try and encourage MG into taking a video of herself masturbating. When MG told him that she can't and that it isn't appropriate for her age, he replied "Age doesn't matter, I know you can do this." Jacobauditions then suggested that they both masturbate together on camera. He requested MG's e-mail address so that he could send her a link to watch him masturbate but she refused to provide it. At that point Jacobauditions sent her a Google hangouts link and advised her to click on it. When she advised that she could not access the link because she does not have a Google account, Jacobauditions advised her to use the e-mail address blakegray2323@gmail.com and gave her a password to access it. When MG questioned this, Jacobauditions responded "that is one of my gmail accounts and passwords." MG advised that she was unable to access the link using the e-mail account and password that he has sent her and he responded multiple times encouraging her to try again. When MG was still unable to access the account, the conversation ended.

47. On September 12, 2018, law enforcement officials in Switzerland were contacted by MG's parents after they learned of the communication with Jacobaudtions and the images and videos that MG created and distributed to him. The parents informed law enforcement of the communications and their daughter's date of birth, which they confirmed to be July of 2008. At this time they also provided their daughter's cellular phone to law enforcement. An extraction report was completed on MG's cell phone and the conversation between she and Jacobauditions as well as several of the images and videos that MG created and distributed were recovered.

48. Swiss investigators contacted Twitter, Inc. regarding their investigation and Twitter subsequently suspended the account "Jacobauditions" and forwarded a Cypbertip complaint to the National Center for Missing and Exploited Children ("NCMEC"). After receiving preliminary information that the subject utilizing the Twitter username "Jacobauditions" was located in the United States, Swiss authorities contacted the FBI for assistance, and provided the information reported by MG's parents and recovered from her phone.

49. The Cybertip report provided by Twitter to the NCMEC was able to provide the following information regarding the account:

Email Address:	jsart1981@mail.com
Screen/User Name:	Jacobauditions
Profile URL:	https://twitter.com/Jacobauditions
IP Address:	66.213.109.2 (Registration) 09-11-2018 10:49:43 UTC
IP Address:	66.213.109.2 (Login) 09-17-2018 12:13:57 UTC
IP Address:	194.59.251.158 (Login) 09-14-2018 13:56:13 UTC
IP Address:	194.59.251.215 (Login) 09-13-2018 18:05:11 UTC
IP Address:	194.59.251.154 (Login) 09-12-2018 20:21:10 UTC
IP Address:	194.59.251.83 (Login) 09-11-2018 18:10:49 UTC

50. IP address 66.213.109.2 is resolved to the Ohio Public Library Information Network in Columbus, OH. Further research indicated that this IP address is specifically linked to Worthington Public Libraries in Worthington, Ohio. Worthington Public Libraries has three locations in Worthington and Columbus, Ohio. On November 27 and November 30, 2018 your

affiant travelled to all three of these locations and accessed the building's publicly available Wi-Fi network utilizing a mobile device and confirmed that the IP address for these buildings is 66.213.109.2.

51. The four IP addresses listed in Paragraph 50 that were provided by Twitter in the Cybertip report beginning with 194.59.251 all resolve to M247 Limited. On September 21, 2018, a subpoena was served on M247 Limited requesting subscriber information for all four IP addresses for the listed dates and times. On September 24, 2018, the investigator who made the request was contacted by legal counsel for M247 Limited who advised that no subscriber information was available because those IP addresses are associated with a Virtual Private Network (VPN). A VPN allows subjects to connect to another network and hides the subject's real IP address by granting them a new IP address from the VPN provider. When a subject connects to a VPN network, the data that the subject transmits is encrypted and transmitted through a secure private channel which provides security, privacy and anonymity.

52. A subpoena was issued to Google, Inc. for any available information regarding the e-mail address blakegray2323@gmail.com. On or about October 23, 2018, Google responded with the following information:

Name:	Blake Gray
E-Mail:	blakegray2323@gmail.com
Created on:	2018/02/08 16:22:19 UTC
Terms of Service IP:	184.58.108.48 on 2018/02/08 16:22:19 UTC
No user IP logs data	

53. IP address 184.58.108.48 is resolved to Spectrum with a geographical location of Blacklick, OH. A subpoena was issued to Time Warner Cable/Spectrum requesting subscriber information for IP address 184.58.108.48 on 2018/02/08 at 16:22:19 UTC. On November 2, 2018, Time Warner Cable/Spectrum responded with the following information:

Name:	Darren KAMNITZER
Address:	699 Streamwater Drive
	Blacklick, OH 43004

54. A search of several publicly available internet websites revealed that Darren KAMNITZER is listed as the Network Administrator for Worthington Public Libraries. Your affiant met with an administrator of the Worthington Public Libraries who confirmed that KAMNITZER is employed as the Network Administrator. In addition, the administrator confirmed that KAMNITZER was at

work on September 11 and September 17, 2018. which is when the Twitter account "jacobauditions" was first registered and again accessed via the IP address linked to and accessible at Worthington Public Libraries.

55. A subpoena was issued to 1&1 Mail & Media, Inc. requesting any identifying or subscriber information for the e-mail address jsart@mail.com. On November 15, 2018, 1&1 Mail responded with the following information:

First/Last Name:	Jacob Sartorius
Registration Date:	2018-09-11 12:48
Date of Birth:	1981-01-01
Last Success Logins:	66.213.109.2 2018-09-17 10:52:41

	IP	Access Time	Success	Reason	Login Type
Logins History:	66.213.109.2	2018-09-17 12:52:41		ha-acs	
	10.74.5.4	2018-09-11 08:49:04		ha-acs	

IP address 10.74.5.4 is a private IP address and no identifying information could be obtained regarding it. As indicated above, IP address 66.213.109.2 is resolved to the Ohio Public Library Information Network, and is specifically linked to Worthington Public Libraries, where Darren KAMNITZER is employed.

56. On January 10, 2019, a federal search warrant was executed at KAMNITZER's residence, 699 Streamwater Drive Blacklick, OH. KAMNITZER was at the residence at the time the search warrant was executed, and agreed to speak to officers. KAMNITZER denied any knowledge of the Jacobauditions Twitter account, or the email account blakegray2323@gmail. KAMNITZER also stated that he did not believe any evidence of child pornography or the sexual exploitation of children would be present on any computers in the house.

57. Pursuant to the search warrant 23 computers and other digital media were seized from the residence and transported to the FBI Columbus Resident Agency, located at 425 W. Nationwide Blvd, Columbus, Ohio 43215. One of the items seized was the SUBJECT MEDIA, which was confirmed to belong to KAMNITZER.

58. A forensic examination of a custom-built desktop computer, which KAMNITZER acknowledged as belonging to and utilized by him, was found to have hundreds of images of child pornography. In addition, a forensic examination of another desktop computer recovered from the residence had additional images and videos of child pornography. Some of these files appeared to

depict prepubescent females in scenes similar to the videos MG was directed to produce by the user of the jacobauditions Twitter account, as described above. Specifically, one of the images depicted a nude prepubescent female bent over and spreading her buttocks. Some of these images were thumbnails located in the cache folder, which indicates that the image or video file related to the thumbnail was viewed on the device at some point, while others were recovered from unallocated space, indicating that they had once been present on the devices but had been deleted. In addition, your affiant utilized forensic software to search for any references anywhere on the devices to "blakegray2323" or the name Jacob Sartorious. The forensic software located thousands of references to the term "blakegray2323" in numerous different folders and locations on one of the computers. Some of these references included indications that the inbox for the blakegray2323@gmail.com account had been accessed from this computer. The forensic software also located numerous references to various Twitter accounts utilizing the last name "Sartorious" as well as Bing searches related to Jacob Sartorious.

59. On or about January 10, 2019, a forensic examination was attempted on the SUBJECT MEDIA. The forensic examination took place at the FBI Columbus Resident Agency and was performed using Cellebrite 4 PC. Although the Cellebrite software was able to extract some information from the SUBJECT MEDIA, this particular model of iPhone will not allow for the type of extraction that recovers deleted data. As discussed above, the chip-off process that the BCI can conduct may potentially recover such deleted data.

60. In light of all of the foregoing information, specifically that: the two identified IP addresses that were utilized to exploit MG are both connected to KAMNITZER; one of those IP addresses is assigned to KAMNITER's employer and thus was likely accessed via a mobile device; KAMNITZER has a background in information technology; there was evidence related to the exploitation of MG (and potentially other minor females) recovered from KAMNITZER's computers; and such evidence had been deleted, your affiant believes that there is a significant likelihood that KAMNITZER utilized the SUBJECT MEDIA to exploit MG and other minor females. Your affiant therefore believes that additional forensic examination of the SUBJECT MEDIA, including conducting a chip-off examination, will produce evidence of the crimes under investigation as well as other child pornography and/or child exploitation offenses.

VIII. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

61. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the seeking, receiving and collecting child pornography, as well as those who seek to sexually exploit children:

A. Those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

B. Those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, often times possess and maintain any "hard copies" of child pornographic material that may exist B that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

D. Likewise, those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the

collector to view the collection, which is valued highly. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted, as described in paragraphs 17 and 18 above.

E. Those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

F. Those who seek out, receive and collect child pornography, as well as those who seek to sexually exploit children, prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

G. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

62. Based upon the conduct of individuals involved in the collection of child pornography set forth in the above paragraph, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of producing, advertising, receiving and possessing child pornography, and coercion or enticement of a minor are currently located in the SUBJECT MEDIA.

IX. CONCLUSION

63. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 2422(b) have been committed, and evidence of those violations are located in the SUBJECT MEDIA. Your affiant respectively requests that the Court issue a search warrant authorizing the search of the SUBJECT MEDIA and the seizure of the items listed in Attachment A.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 4th day of February 2019.

Elizabeth Preston-Deavers
United States Magistrate Judge
United States District Court, Southern District of Ohio

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252, 2252A and 2422(b).

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or communications programs), utilities, compilers, interpreters, and communications programs.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, letters, e-mail messages, chat logs, electronic messages, other digital data files and web cache information) pertaining to the production, possession, receipt, or distribution of child pornography.

3. In any format and medium, all originals, computer files, copies, and negatives of child pornography or child erotica.

4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between Darren Kamnitzer, and any of his alias, including, but not limited to, Jacobauditions and Blake Gray, and any other individuals related to the sexual abuse or exploitation of minors.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

8. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered.

ATTACHMENT B
DESCRIPTION OF PLACE TO BE SEARCHED

1) Apple Iphone Model MNAY2LL/A with internal serial number of F71T89YMHG6W that was recovered in the garage of Darren Kamnitzer's residence, pursuant to a federal search warrant, located at 699 Streamwater Drive Blacklick, OH 43004.